

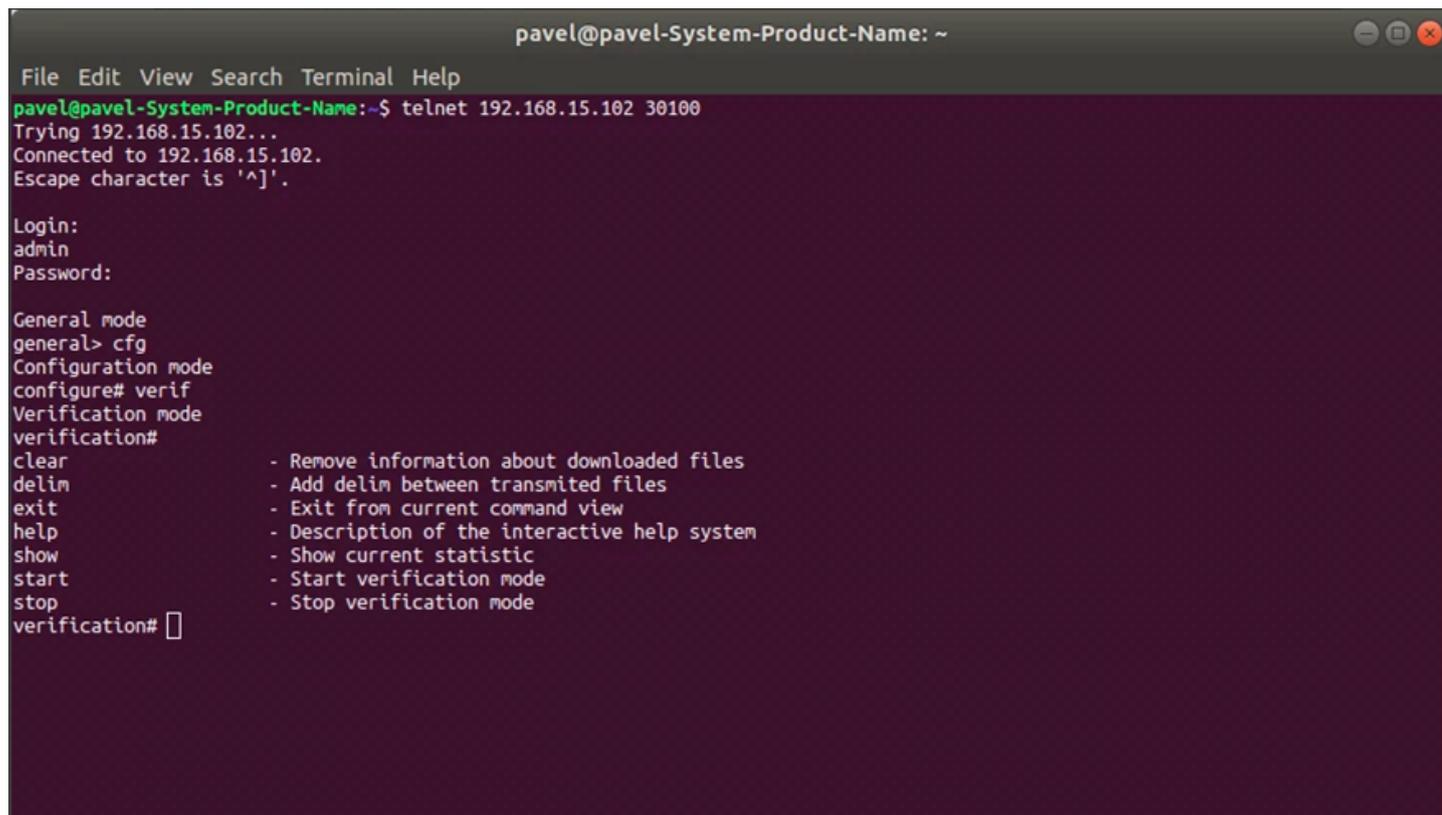
# Режим поверки зондов WPE-103 и WPE-108

Режим поверки реализован для осуществления поверки измерительным комплексом «ВЕКТОР ИКИ».или "АМУЛЕТ"(в случае однопортового зонда sheeva)

## Реализация

Проверка прибором "ВЕКТОР ИКИ" Реализована с помощью iptables и утилиты ulog-acctd. Проверка "АМУЛЕТ" использует "сырые" сокеты для получения данных о переданной информации на зонд.

Для осуществления поверки добавлен новый режим **verification** в пользовательский telnet. Для того чтобы зайти в этот режим, необходимо обладать правами, не ниже admin. Переключение в режим поверки происходит из режима конфигурации, при вводе verification.



```
pavel@pavel-System-Product-Name: ~
File Edit View Search Terminal Help
pavel@pavel-System-Product-Name:~$ telnet 192.168.15.102 30100
Trying 192.168.15.102...
Connected to 192.168.15.102.
Escape character is '^]'.

Login:
admin
Password:

General mode
general> cfg
Configuration mode
configure# verif
Verification mode
verification#
clear                - Remove information about downloaded files
delim                - Add delim between transmited files
exit                 - Exit from current command view
help                 - Description of the interactive help system
show                 - Show current statistic
start                - Start verification mode
stop                 - Stop verification mode
verification#
```

Рисунок 67 — Список команд в режиме поверки

## Описание команд

- clear — записывает вектор информации о переданных файлах в текстовый документ (/var/log/slamon.%Y%m%d-%H-%M-%S). Затем очищает вектор, в котором содержится.

- `delim` — выполняется после успешной отправки файла. Подсчитывает количество переданной информации, количество пакетов и среднюю скорость.
- `exit` — осуществляет выход из режима проверки.
- `help` — открывает описание интерактивной справочной системы.
- `show` — выводит информацию на текущий момент.
- `start` — запускает `wizard` и подготавливает устройство к проверке. Подробнее в «Выполнение проверки».
- `stop` — останавливает проверку и возвращает устройство в «обычный» режим работы.

## Выполнение проверки

После ввода команды «`start`», «`wizard`» запрашивает данные от пользователя в зависимости от собранной схемы:

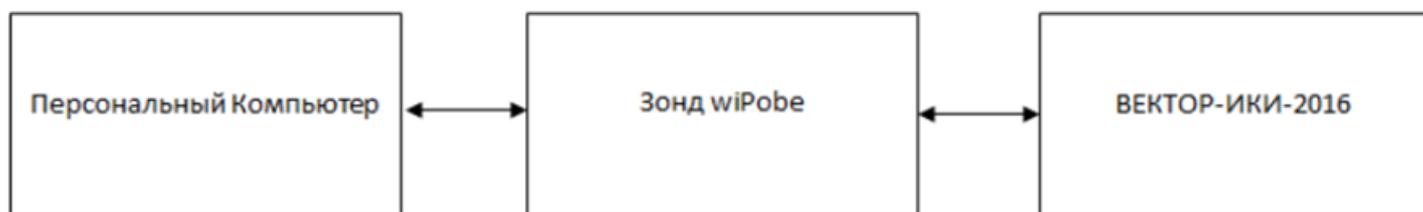


Рисунок 68 — Схема подключения двухпортового зонда

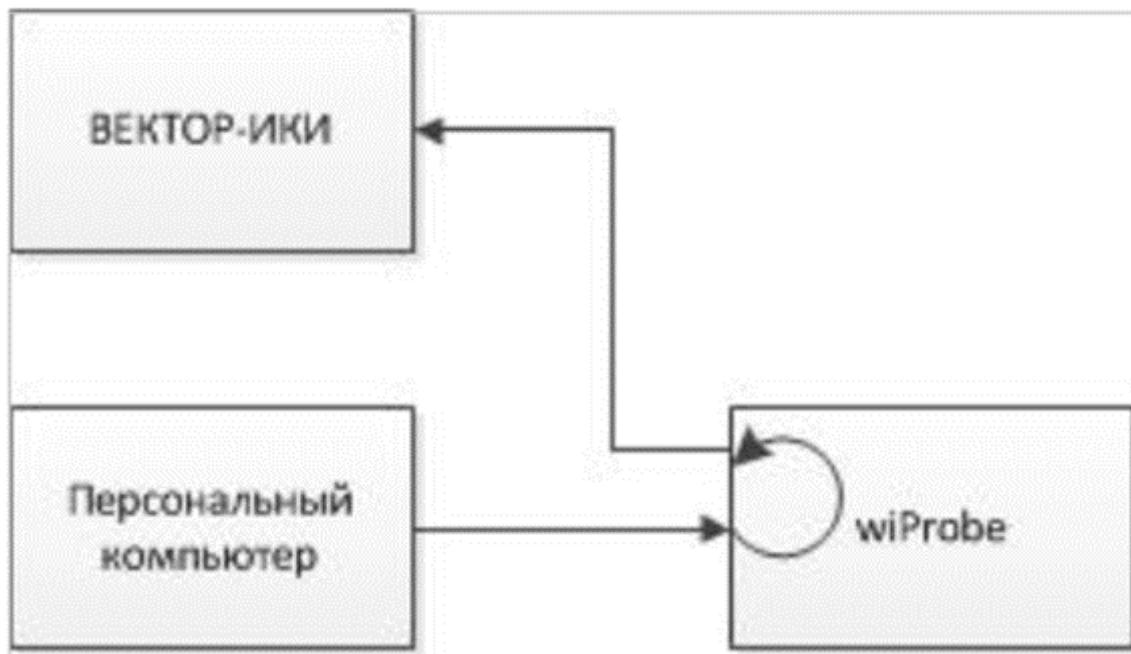


Рисунок 69 — Схема подключения однопортового зонда

Для двухпортового зонда (Рисунок 67) необходимо ввести IP-адрес и порт назначения. Для однопортового зонда (Рисунок 68) — IP-адрес и порт назначения, а также локальный порт для зонда `wiProbe`, на который будут посылаться данные.

```
pavel@pavel-System-Product-Name: ~  
File Edit View Search Terminal Help  
pavel@pavel-System-Product-Name:~$ telnet 192.168.15.125 30100  
Trying 192.168.15.125...  
Connected to 192.168.15.125.  
Escape character is '^]'.  
  
Login:  
admin  
Password:  
  
General mode  
general> cfg  
Configuration mode  
configure# ver  
Verification mode  
verification# start  
Input destination ip address  
192.168.15.122  
Input destination port:  
5021  
Input wiprobe port:  
5066  
Verification start...  
verification#
```

Рисунок 70 — Пример запуска проверки зонда

На рисунке 69 (схема собрана для однопортового зонда, как указано на рисунке 68) в качестве «Вектор-ИКИ» выступает хост с адресом 192.168.15.122:5021, у зонда wiProbe адрес 192.168.15.125. После ввода необходимых данных приостанавливается сетевая активность зонда и запрещается изменение данных из конфигурационного режима пользовательского telnet. Также сохраняется состояние iptables и добавляются новые правила для фиксации проходящего трафика.

Согласно схеме, персональный компьютер должен отправлять данные не напрямую «Вектор-ИКИ», а на порт 5066 зонда wiProbe. Зонд, в свою очередь, пересылает весь трафик, с порта 5066 на «Вектор-ИКИ», собирая необходимую информацию.

Пользователь, проводящий проверку зонда, в интерфейсе «Вектор-ИКИ» выбирает файлы эталонных размеров, которые будет передавать.

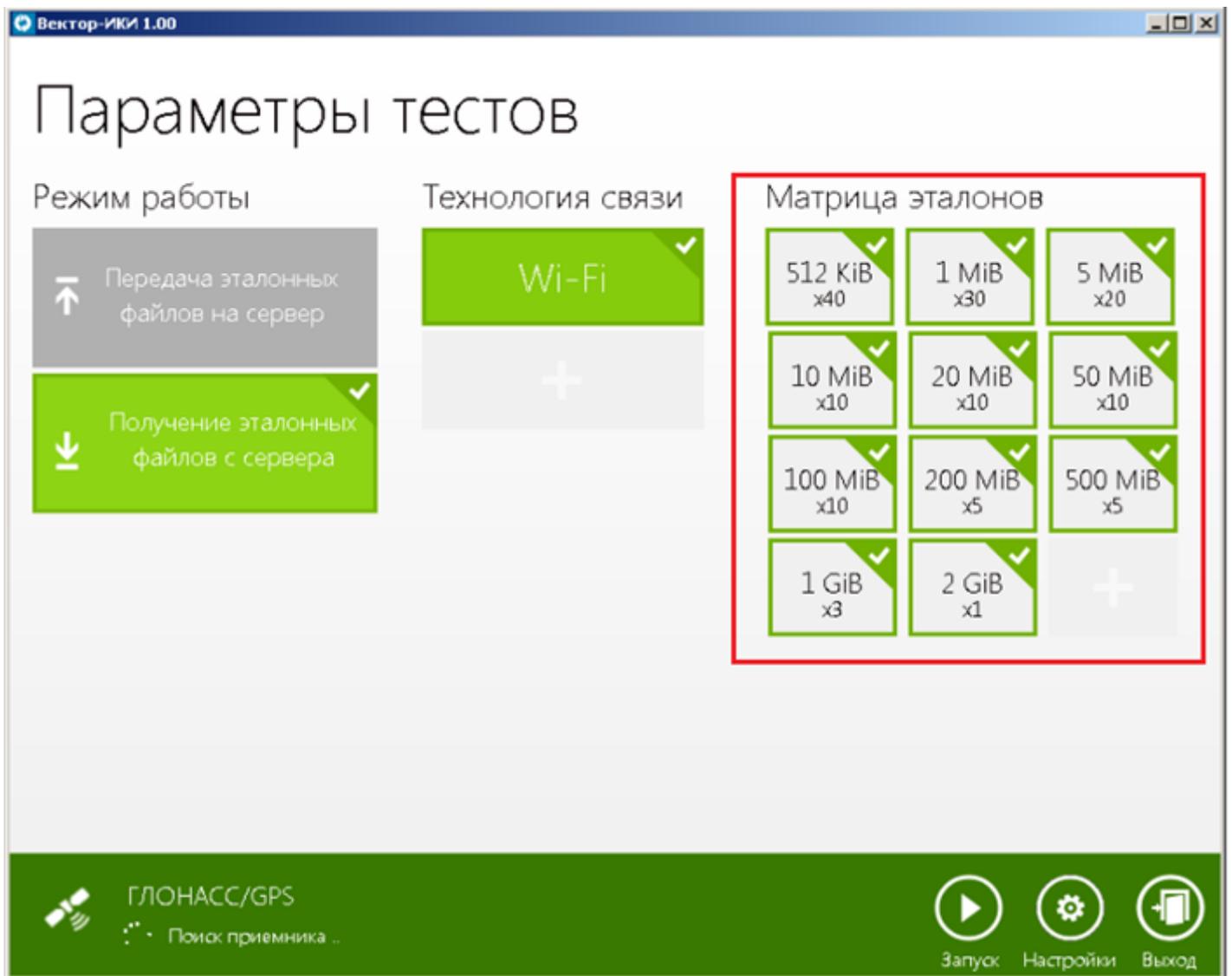


Рисунок 71 — Интерфейс измерительного комплекса «Вектор-ИКИ», в котором выбираются файлы эталонных значений для передачи

После запуска измерительного комплекса «Вектор-ИКИ», в течение некоторого времени, осуществляется передача файлов с эталонными размерами. После окончания передачи, пользователю необходимо ввести команду `delim`, после которой произойдет подсчет следующих параметров:

- количество переданной информации;
- количество переданных пакетов;
- средняя скорость.

Для получения статистики по каждому переданному файлу необходимо передавать файлы по-одному и вводить команду `delim` после каждой передачи.

В качестве примера, будет запущена утилита «iperf», передающая трафик в течении заданного времени:

```

pavel@pavel-System-Product-Name: ~
File Edit View Search Terminal Help
configure# veri
Verification mode
Verification# start
Input destination ip address
    192.168.15.122
Input destination port:
    5021
Input wiprobe port:
    5066
Verification start...
Verification# delim
Waiting 5 seconds...
Command successfully executed
Verification# delim
Waiting 5 seconds...
Command successfully executed
Verification# sh
Iter   Bytes          Packets    Aver. speed  Duration    Flow started    Flow ended
1(tx)  119214132(113 MB)  79479     90.9532 MBits/s  10          2019.07.08-12-29-43  2019.07.08-12-29-53
      (rx)  2055516(1 MB)    39529     ---          10          2019.07.08-12-29-43  2019.07.08-12-29-53
2(tx)  261782124(249 MB)  174525    90.7836 MBits/s  22          2019.07.08-12-30-06  2019.07.08-12-30-28
      (rx)  4497592(4 MB)    86492     ---          22          2019.07.08-12-30-06  2019.07.08-12-30-28
Verification#

```

```

pavel@pavel-System-Product-Name: ~
File Edit View Search Terminal Help
pavel@pavel-System-Product-Name:~$ iperf -c 192.168.15.125 -p 5066
-----
Client connecting to 192.168.15.125, TCP port 5066
TCP window size: 325 KByte (default)
-----
[ 3] local 192.168.14.184 port 47654 connected with 192.168.15.125 port 5066
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-10.0 sec  110 MBytes  92.0 Mbits/sec
pavel@pavel-System-Product-Name:~$ iperf -c 192.168.15.125 -p 5066 -t 22
-----
Client connecting to 192.168.15.125, TCP port 5066
TCP window size: 325 KByte (default)
-----
[ 3] local 192.168.14.184 port 47658 connected with 192.168.15.125 port 5066
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-22.0 sec  241 MBytes  91.8 Mbits/sec
pavel@pavel-System-Product-Name:~$

```

```

pavel@pavel-System-Product-Name: ~
File Edit View Search Terminal Help
sheevaplug-debian:~# iperf -s -p 5021
-----
Server listening on TCP port 5021
TCP window size: 1.33 MByte (default)
-----
[ 4] local 192.168.15.122 port 5021 connected with 192.168.15.125 port 47654
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-10.1 sec  110 MBytes  91.3 Mbits/sec
[ 5] local 192.168.15.122 port 5021 connected with 192.168.15.125 port 47658
[ 5] 0.0-22.1 sec  241 MBytes  91.4 Mbits/sec

```

Рисунок 72 — Пример вывода режима проверки зонда wiProbe

## Описание примера

В левом нижнем терминале запущен пользовательский telnet с зондом wiProbe (192.168.15.125). В правом нижнем терминале — зонд с адресом 192.168.15.122. Верхний терминал — это персональный компьютер на схеме.

Персональный компьютер (верхний терминал) генерирует трафик в течении 10 секунд на первой итерации, отправляя его на адрес 192.168.15.125:5066. wiProbe заворачивает его на адрес 192.168.15.122:5021 и анализирует. После того, как пройдет 10 секунд, вводится команда `delim`. Ожидание в течение 5 секунд, о котором сообщается в выводе, необходимо чтобы данные о нагрузке на сетевом интерфейсе передались в пространство пользователя. После чего, для просмотра результатов анализа проходящего потока данных, можно ввести команду `show`.

Формат вывода: Iter (номер файла, для которого выполнялась команда `delim`, подпись потока (прямой и обратный)), Bytes (количество переданных байтов), Packets (количество переданных пакетов), Aver. Speed (средняя скорость) и Duration (длительность передачи), Flow started (время начала передачи), Flow ended (время окончания передачи). На второй итерации `iperf` генерирует трафик в течение 22 секунд, затем все действия повторяются в telnet. Таким образом, каждый замер добавляется в вектор результатов.

Завершение проверки происходит с помощью ввода команды `stop`. Она возвращает iptables в изначальное состояние и восстанавливает сетевую активность устройства

# Описание действий wiProbe при начале проверки

## Команда `start`

После получения команды `start` зонд сохраняет конфигурацию iptables, а затем добавляет новые правила. Для однопортового зонда:

```
iptables
```

```
iptables -t nat -A PREROUTING --dst 192.168.15.125 -p tcp --dport 5010 -j DNAT --to-destination 192.168.15.122:5011
```

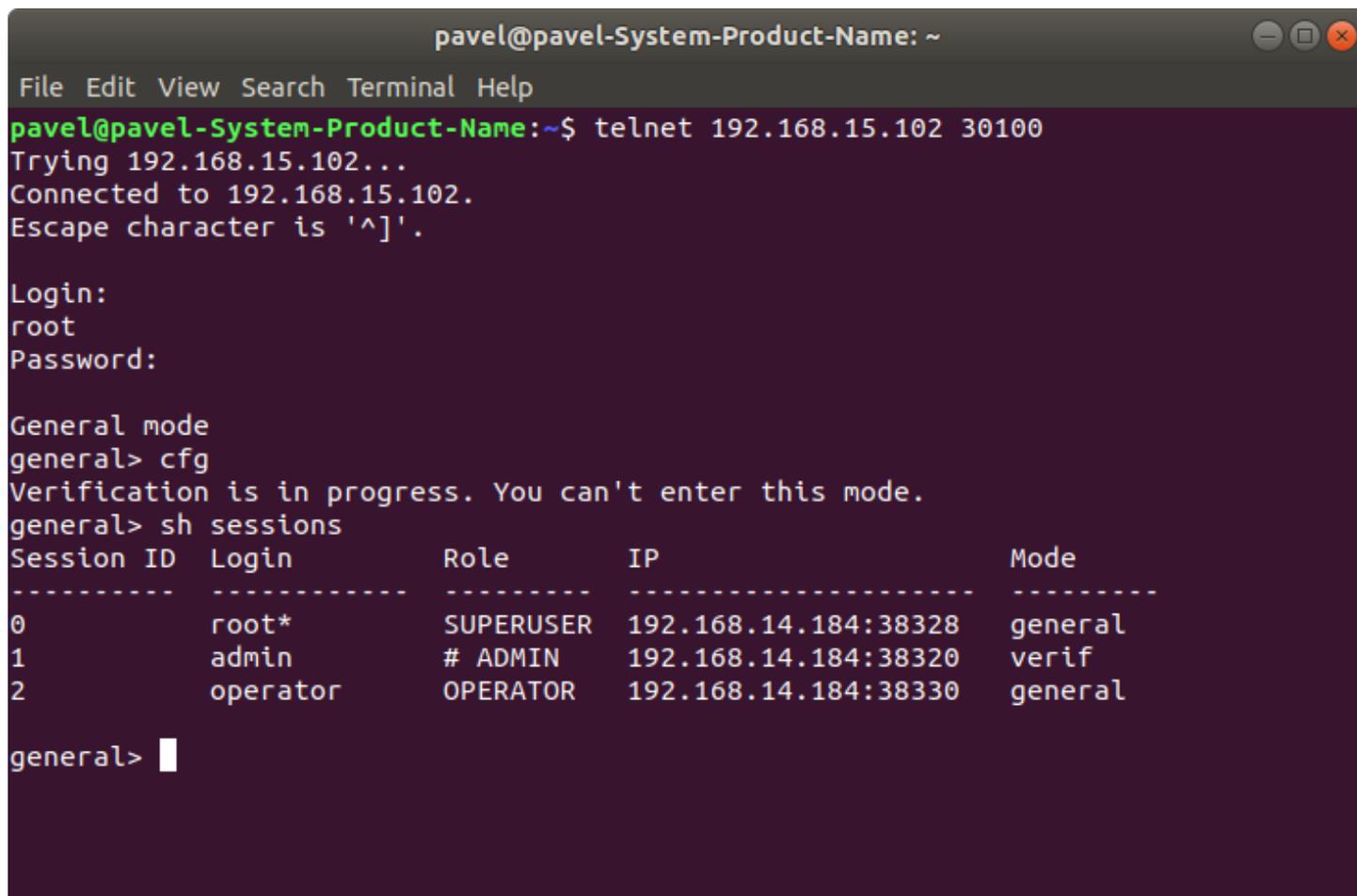
```
iptables -I FORWARD 1 -i eth0 -o eth0 -d 192.168.15.122 -p tcp -m tcp --dport 5011 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING --dst 192.168.15.122 -p tcp --dport 5011 -j SNAT --to-source 192.168.15.125
```

```
iptables -I FORWARD 1 -i eth0 -o eth0 -j ULOG --ulog-cprange 48 --ulog-qthreshold 50
```

В соответствии с приведенными правилами, все tcp-сегменты, пришедшие на порт 5010 зонда с адресом 192.168.15.125 будут перенаправлены на адрес 192.168.15.122:5011. Второе правило разрешает проброс пакетов на интерфейсе «eth0» к адресу 192.168.15.122. Третье правило подменяет адрес источника, чтобы пакеты также возвращались 125-му зонду, а не напрямую источнику. Четвертое правило копирует и передает в пространство пользователя первые 48 байт каждого пакета, накапливает информацию о 50 пакетах, прежде чем отправить информацию.

После этого отправляется команда модулю slamon, о приостановке сетевой активности (PAUSE\_NETWORK\_ACTIVITY) и захват блокировки сессией telnet. Другие пользователи не смогут войти в режим конфигурирования. Попытка войти в режим конфигурирования пользователем, обладающим блокировкой, переведет его обратно в режим верификации.



```
pavel@pavel-System-Product-Name: ~  
File Edit View Search Terminal Help  
pavel@pavel-System-Product-Name:~$ telnet 192.168.15.102 30100  
Trying 192.168.15.102...  
Connected to 192.168.15.102.  
Escape character is '^]'.  
  
Login:  
root  
Password:  
  
General mode  
general> cfg  
Verification is in progress. You can't enter this mode.  
general> sh sessions  
Session ID  Login          Role           IP              Mode  
-----  
0           root*          SUPERUSER     192.168.14.184:38328  general  
1           admin          # ADMIN       192.168.14.184:38320  verif  
2           operator       OPERATOR      192.168.14.184:38330  general  
  
general> █
```

Символ «#» в столбце «Role», означает, что этот пользователь начал верификацию.

## Команда `delim`

Каждая запись `ulog-acctd` имеет вид в соответствии с строкой форматирования (`%s\t%d\t%S\t%D\t%b\t%P\t%x\t%\n`(из файла `/etc/ulog-acctd.conf`):

`account.log`

source IP	dest IP	source port	dest port	bytes	packets	since	till
192.168.14.184	192.168.15.125			47658		7788	123151772 82105
1562037132	1562037142						
192.168.15.125	192.168.14.184			7788		47658	3125337 32403
1562037132	1562037142						
194.190.168.1	192.168.15.125			42832		123	76 1
1562037144	1562037144						
192.36.143.130	192.168.15.125			55453		123	76 1
1562037146	1562037146						
91.207.136.55	192.168.15.125			48632		123	76 1
1562037146	1562037146						
194.190.168.1	192.168.15.125			47627		123	76 1
1562037176	1562037176						
192.36.143.130	192.168.15.125			54658		123	76 1
1562037178	1562037178						
91.207.136.55	192.168.15.125			51484		123	76 1
1562037178	1562037178						

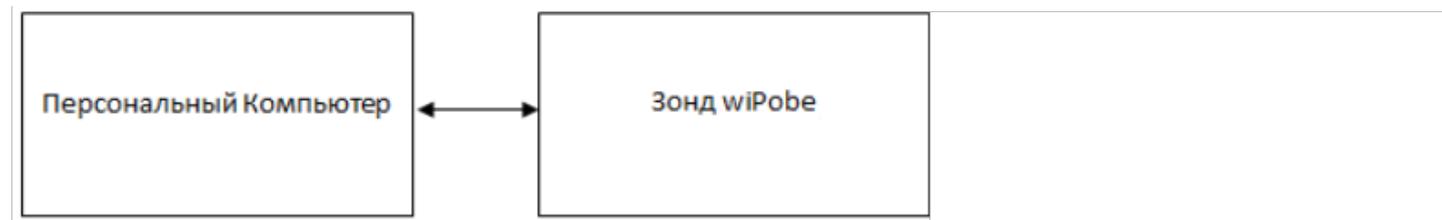
По адресу и порту назначения выбирается необходимый для анализа поток. Количество переданных байт, пакетов и длительность записываются в вектор. Поскольку время начала потока и окончания записывается в секундах, то существует следующая проблема: если начало передачи пришлось на  $\sim 0.96$  секунды, а окончание на  $\sim 11.02$  секунды, то доли секунды будут отброшены, и длительность составит 11 с, хотя на самом деле была 10.06 с.

## Команда `stop`

После этой команды зонд возвращает состояние `iptables` к тому, которое было перед началом проверки. Также выполняется команда восстановления сетевой активности (`RESTORE_NETWORK_ACTIVITY`).

## Проверка с помощью "Амулет"

Схема:



После ввода команды `start`, wizard запрашивает данные от пользователя и запускает процесс подсчета полученных и переданных данных

```
root@mikhail-zolotukhin: /etc
Connection closed by foreign host.
root@mikhail-zolotukhin:/etc# telnet 192.168.15.125 30100
Trying 192.168.15.125...
Connected to 192.168.15.125.
Escape character is '^]'.

Login:
admin
Password:

General mode
general> cfg
Configuration mode
configure# verification
Verification mode
verification# start
Please, choice type of verification: V(Vector) or A(Amulet):
A
Please, enter interface name
eth0
Input destination ip address
192.168.15.121
Verification start. You may see current result by command 'show' and stop verification using 'stop'
verification#
```

## Команда `show`.

С помощью команды `show` можно посмотреть текущую статистику по полученным/отправленным данным.

```
root@mikhail-zolotukhin: /etc
verification# start
Please, choice type of verification: V(Vector) or A(Amulet):
A
Please, enter interface name
eth0
Input destination ip address
192.168.15.121
Verification start. You may see current result by command 'show' and stop verification using 'stop'
verification# show
Listen at eth0
Mirror to 192.168.15.121
3:31:40:811 size 76 data 56 src {192.36.143.130} dst {192.168.15.125} Send 84
3:31:40:992 size 52 data 32 src {192.168.14.187} dst {192.168.15.125} Send 60
3:31:41:356 size 53 data 33 src {192.168.14.187} dst {192.168.15.125} Send 61
3:31:41:357 size 52 data 32 src {192.168.14.187} dst {192.168.15.125} Send 60
3:31:41:524 size 53 data 33 src {192.168.14.187} dst {192.168.15.125} Send 61
3:31:41:525 size 52 data 32 src {192.168.14.187} dst {192.168.15.125} Send 60
3:31:41:808 size 76 data 56 src {91.207.136.50} dst {192.168.15.125} Send 84
3:31:41:868 size 53 data 33 src {192.168.14.187} dst {192.168.15.125} Send 61
3:31:41:869 size 52 data 32 src {192.168.14.187} dst {192.168.15.125} Send 60
3:31:42:60 size 53 data 33 src {192.168.14.187} dst {192.168.15.125} Send 61
3:31:42:61 size 52 data 32 src {192.168.14.187} dst {192.168.15.125} Send 60
verification#
```

## Команда `stop`.

После команды `stop` текущая проверка заканчивается. Команда `show` после этого будет показывать статистику по прошедшей проверке.

## Команда `exit`.

Делает выход из режима проверки.

---